Initial Security Management Plan

Sefton Council

August 2018

Version: 0.2

At Agilisys we deliver success through innovation… working with our clients to transform services that make a difference to millions of people across the UK

AGILISYS

Third Floor, One Hammersmith Broadway, Hammersmith, London, W6 9DLP 0845 450 1131 F 0845 450 1132 info@agilisys.co.uk

www.agilisys.co.uk

Table of Contents

Glossary

Abbreviation	Meaning
BPSS	Baseline Personnel Security Standard
CESG	Communications Electronics Security Group
HMG	Her Majesty's Government
ISMS	Information Security Management System
ITIL	IT Infrastructure Library (now renamed IT Lifecycle Management Process)
PDCA	Plan-Do-Check-Act: The Deming Cycle
SoA	Statement of Applicability
SMP	Security Management Plan
SSC	Security Steering Committee

References

Ref	Artefact/Reference
001	ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.
002	ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management.

1 Introduction

This document is the Security Management Plan for Agilisys' services delivered to Sefton MBC (the Council).

This document is intended to be a live, working document for the duration of the contract with the Council. It will be regularly reviewed and the content the narrative within updated to reflect changes of note throughout the contract term.

The document describes how Agilisys manages information security which is according to leading industry practice and specifies any **additional or different application of controls**, specifically required due to the nature of Agilisys' services to the Council.

1.1 Purpose

The purpose of this document – the Security Management Plan (SMP) is as follows:

- Define the scope and boundaries of the Agilisys Information Security Management System (ISMS);
- Documented commitment by Agilisys management to a fit-for-purpose ISMS;
- Documented roles and responsibilities within Agilisys for the ISMS
- Description of the major elements governing the implementation and operations of the ISMS that is required for compliance against ISO/IEC 27001:2013 standard.

The governance of the security management programme will be conducted according to leading industry practice. The security management of individual programme elements will meet the Council's obligations to protect sensitive information assets and to assess and report on compliance with mandatory minimum requirements for information assurance.

1.2 Scope

This document will define the content and structure of the Agilisys ISMS and on-going maintenance. The SMP will record the plan to implement the components, structure and documentation requirements of the ISMS.

It will also address the requirements for staff, processes, documentation, technology and physical facilities needed to meet the specific information security, governance and assurance requirements of the Council and will document how these additional requirements are to be added to the Agilisys ISMS.

The SMP is not intended to define or document the operational processes, procedures, or associated work instructions or documentation records to be deployed for the Council, but to identify the areas in which these detailed artefacts are to be delivered. The position of the SMP in the overall ISMS framework and security policy/ governance document set is shown in the figure below. As the SMP is the top-level document, it refers out to other documents rather than reproducing their content.

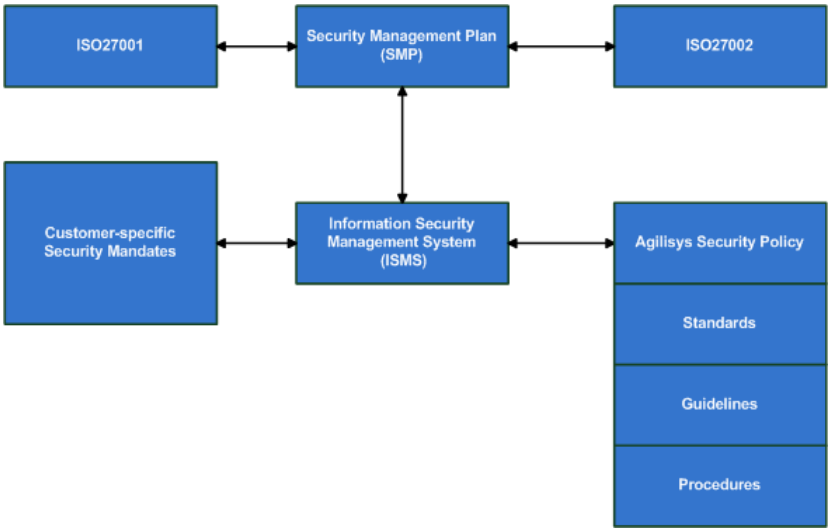

Figure 1: Scope of Security Management Plan

1.3 ISMS Objectives

The objective of the ISMS is to align Agilisys' approach to information security management to ISO 27001:2013.

The ISMS is a continuous process and will be maintained through the Plan, Do, Check and Act (PDCA) cycle as defined by the standard.

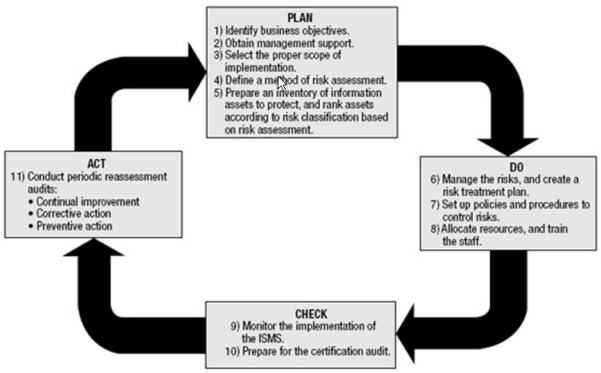

Figure 2: Plan, Do, Check and Act (PDCA) cycle Plan

The ISMS will help to ensure that appropriate controls are implemented to mitigate information security risks at a level commensurate with the value of the information, and in line with best practices suggested in ISO/IEC 27001 as well as ISO/IEC 27002.

1.4 ISMS Security Controls

The following figure represents the structure of the ISMS to be implemented.

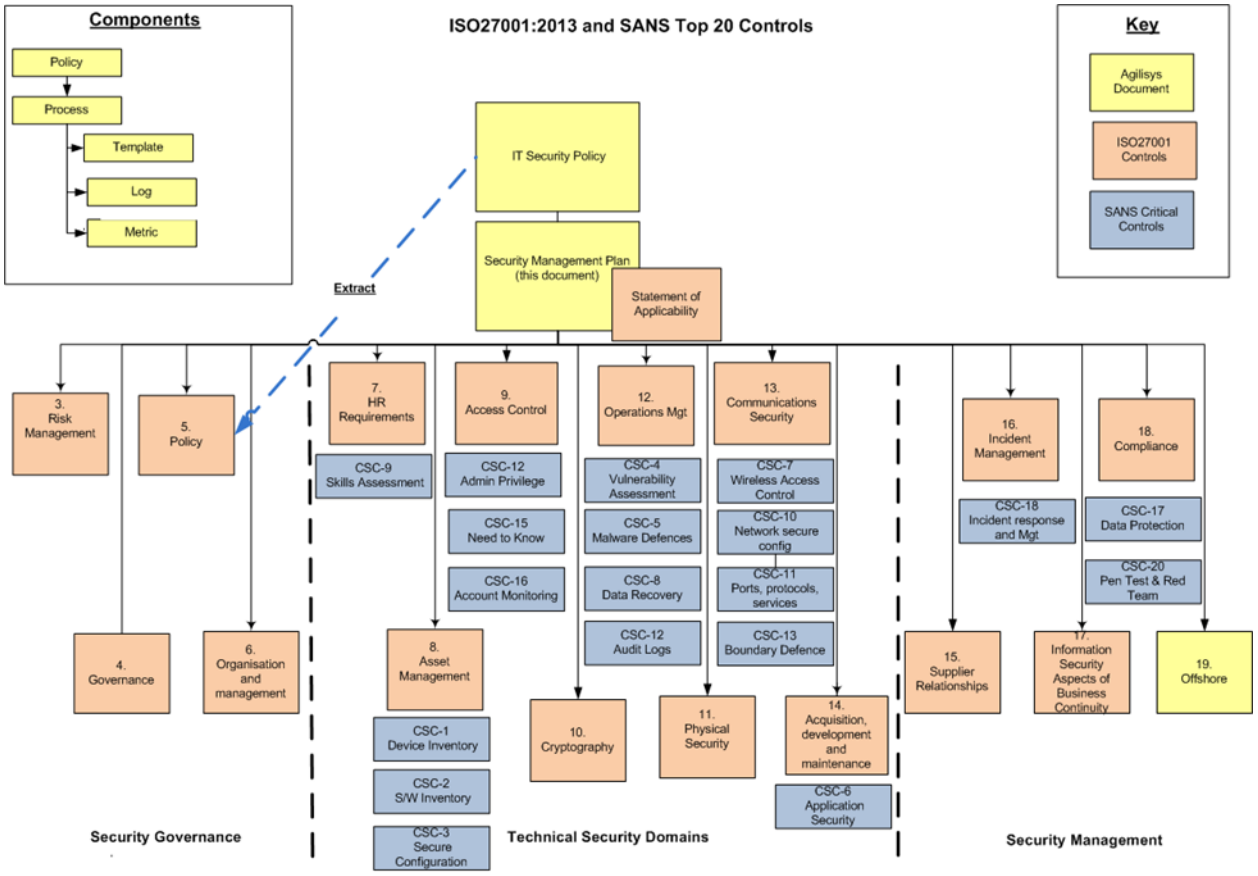

Figure 3: ISMS security controls

The structure follows the naming and numbering convention in Annex A of ISO27001:2013. Within each of the security domains, groups of controls to support one or more control objectives are derived from:

- **Business controls**: These represent the standard set of security controls applied to every Agilisys solution.
- **ISMS Controls**: These represent the additional controls required to complete the ISO27001 Statement of Applicability.
- **QMS Controls**: These represent re-use of standard functions for document and records management, taken from the Agilisys Quality Management System (QMS).

The elements to which Agilisys will apply the ISMS controls and which are **specific only** to the services provided by Agilisys to the Council and the associated environment include.

- Locations
- Teams (including staff to be transferred under TUPE, if applicable)
- Business processes (to be defined)
- Applications (to be defined)

1.5 Implementation & Transition

During the Implementation phase (and post Transition), the Security Management Plan (SMP) will be developed further in close collaboration with the Council, in accordance with a mutually agreed timetable to ensure all risks are identified and understood. As part of Implementation, this will typically include, but not limited to, the following:

- Working collaboratively with the Council to establish a joint Sefton Council/Agilisys Information Security Forum, the Security Steering Committee (SSC) (with agreed Terms of Reference) to oversee the evolution of, and delivery of, information security in accordance with the relevant requirements. The Joint Information Security Forum will
  - Provide the governance to oversee the Implementation
  - Ensure there is clarity regarding the management roles and responsibilities in each organisation
  - Agree the ongoing roles and responsibilities for information security compliance
  - Establish a schedule of regular meetings
    - The initial meetings will be held at least once a month and more frequently if necessary. This could be reduced to quarterly meetings once the new arrangements have bedded down but any changes to the schedule of meetings will only be implemented if they have been agreed with the Council
- Undertaking a gap analysis of the controls in place at on-boarding and those required for service delivery to the Council against the controls Agilisys uses to ascertain current state, identify unmanaged risks and plan for improvement activities
- Based on this analysis, integrate (where applicable) the Council's existing security methods, techniques, technologies, etc. into the ISMS
- Undertaking a comparison of the Council's Information Security Policy and related documents with Agilisys security policy documents
- Performing discovery activities to fully understand the security context of services to be provided to the Council
- Through the Joint Information Security Forum deciding if any additionally identified security controls will be added to the ISMS or applied separately
- Preparing the ISMS to include services provided to the Council
- Taking ownership of information security management for services provided to the Council
- Through the Joint Information Security Forum agreeing appropriate security assurance mechanisms, such as an internal audit schedule
- Conducting ongoing information security reviews and risk assessments to identify and/or verify information security requirement
- Agreeing an approach to security classification based on the needs of the Council
- Agreeing the sequence and ownership of actions to implement controls or improvements to bring the security of the services to the Council in line with the requirements

1.5.1 Mobilisation Phase

Agilisys will:

- Perform discovery activities to fully understand the security context of services to be provided to the Council
- Prepare the Agilisys ISMS to include services provided to the Council
- Prepare roles and responsibilities for management and governance of information security
- Establish a schedule of regular meetings of the Agilisys/Sefton Council Joint Information Security Forum

1.5.2 Transition Phase

Agilisys will:

- Take ownership of information security management for services provided to the Council
- Integrate existing Council security methods, techniques, technologies, etc. into the Agilisys ISMS
- Conduct initial internal audits to ascertain current state, identify unmanaged risks and plan for improvement activities
- Conduct information security reviews and risk assessments to identify and/or verify information security requirements.
- Apply transitional governance and management roles and responsibilities.

1.6 On-going Review

The SMP will be reviewed and updated as security policies, processes and standards are implemented.

The SMP, together with the other relevant security documents, will be subjected to regular (at least annually) review by senior management, as part of continuous improvement. This management review will be implemented through:

- The Agilisys/Sefton Council Joint Information Security Forum

1.7 Independent Audit and Certification

ISO 27001

In the event of the Council requiring the ISMS used for Agilisys services delivered to / on behalf of the Council to be independently audited and/or certified as meeting the requirements of ISO 27001:2013), Agilisys will:

- Obtain independent certification of the ISMS to ISO 27001 within a period as defined and agreed with the Council

An approach to undertake this will be jointly agreed with the Council and will include:

- The sequence of services transitioning to Agilisys control;
- Whether the required time period for certification allows sufficient time to gather a complete cycle (assume minimum of 3 months) of evidence from the ISMS and security processes after the final service is completed via Implementation;
- An internal audit programme for the following 12 months;
- Activities to ensure that an internal audit of all the security controls defined in the *Statement of Applicability* is completed before the certification audit;
- Timing and approach to engage a UKAS Audit Body, including the timing of the Pre-Audit Assessment, the certification audit and Year 2/3 surveillance audits;
- Scope of the certification (if not included in the Agilisys ISMS certification scope);

Certification will be based on the following premises:

- The scope for certification will be the sum of the Agilisys corporate ISMS, together with the additional Council specific elements to be documented in this Security Management Plan.
- Certification will be obtained by completing a full audit cycle to be completed by a UKAS Audit Body, to include:
  - An updated scope statement
  - An updated *Security Management Plan*, including the description of any Council specific security controls (this document)
  - An updated *Statement of Applicability* (SoA).

PCI DSS

In the event that Agilisys undertakes the processing of card payments or passes control to a Payment Processor on behalf of the Council, PCI DSS certification may be required.

Agilisys will comply with the relevant aspects of the Payment Card Industry (PCI) security standards, including those provisions pertaining to call recording, where appropriate. The level of compliance necessary will vary depending on the level of processing undertaken.

An approach to undertake this will be jointly agreed with the Council and will include:

- The sequence of services transitioning to Agilisys control;
- An internal audit programme for the following 12 months;
- Activities to ensure that an internal audit of all the security controls defined in the PCI DSS standard is completed prior to any certification audit;
- Timing and approach to engage a PCI Qualified Security Assessor (where required) to provide guidance, including the timing of any certification audits (where required) and continuing certification cycle;
- Scope of the cardholder data environment;
- Schedule for penetration testing (internal and external) to be carried out by a qualified CHECK or CREST (or equivalent) independent tester;
- Requirements for Agilisys registration as a Service Provider with each of the clients Merchant Acquirer
- Evidence to be provided by Agilisys to the Council to show compliance (e.g. copies of certificates, self-assessment questionnaires, compliance statements and results of security tests as relevant to the level of processing undertaken).

Agilisys will also perform a regular annual internal audit of the technical design to ensure it continues to reflect good security practice, taking into account any new and emerging threats and new technologies.

If Agilisys are required to comply with PCI DSS where payments are being processed, the proposed approach to achieve this PCI DSS compliance is as follows:

- Engage a PCI Qualified Security Assessor (where required) to provide guidance
    - This will be for a number of days (number still to be defined) at the beginning of the project to ensure that our approach is correct and we have assessed ourselves at the correct level
- Complete a gap analysis against the current version of PCI DSS
    - Identify any gaps and activity required to close out those gaps
    - Create an action plan to close out gaps (to be provided to the Council)
- Complete self-assessment questionnaire and Attestation of compliance
- Perform relevant scans and penetration tests (where required)
- Submit self-assessment questionnaire and Attestation of compliance to the relevant payment brand(s) or the Council
- On-going compliance with PCI DSS including regular security testing of the environment in line with the requirements of the PCI DSS Standard (the Council to be informed upon completion of testing, any service impacting weaknesses and plans for mitigation)
- On-going annual completion and submission of self-assessment questionnaire

1.8 Contract Exit

The responsible owner for Information Security, e.g. the Information Security Manager, will be responsible for ensuring continuity of security during the exit period. This responsibility will address both the maintenance

of security functions during handover and also the transfer of security responsibilities to the Council or Replacement Contractor, as appropriate.

The Information Security Manager will:

- Provide security input during preparation of the initial exit plan;
- Conduct regular reviews of the security content of the exit plan as part of the annual ISMS management review;
- Provide specialist assistance to Exit Managers during the termination assistance period;
- Establish attend and facilitate the Joint Information Security Forum with the Council and the Replacement Contractor; and
- Document procedures for the transfer of responsibilities defined in this document to the Council or to the Replacement Contractor.

1.8.1 Cryptographic Key Management

The Information Security Manager will work with the Council and the Replacement Contractor to agree, document, test and schedule a technical solution for handover of any PKI solution addressing:

- Synchronisation of certificate repositories between Agilisys and the Replacement Contractor; and
- Revocation of incumbent Agilisys keys and issue of Replacement Contractor keys to all the Council's systems and devices, to ensure continuity of service.

1.8.2 Sefton Council's Data and Records

The Information Security Manager will define, document and test procedures to allow for the safe transfer of all Council data and records to the Council or to the Replacement Contractor. The process will define:

- Maintenance of the security content in registers of assets, contracts and Intellectual Property;
- Maintenance of an inventory of the Council's data held by Agilisys;
- Export of data from the Agilisys ISMS in a neutral format (e.g. Microsoft Excel), together with a data dictionary, defining the format and structure of the supplied data;
- Security of manual or electronic transfer of the Council's data to the Council or Replacement Contractor; and
- Secure disposal of records and sanitisation of all storage devices, prior to decommissioning.

2 Risk Management

2.1 Risk Assessment / Risk Acceptance

Agilisys shall adopt an approach to risk management based on a combination of qualitative and quantitative processes that follow the framework defined in the ISO/IEC 27005:2008 Information Security Risk Management standard and that meets the requirements of the Agilisys Information Security Risk Management Framework.

At a high level, the ISMS risk assessment process includes the following steps:

- Quarterly workshops involving relevant managers, team leaders, and specialists shall be undertaken to determine/confirm the list of information assets that should be protected under the ISMS, identifying the owner and the classification of each asset.
- Determination of the threat, likelihood and business impact based on the identified information assets to ensure that the risk assessment reflects the realistic view of the business.
- Population and maintenance of an Information Security Risk Register owned and reviewed regularly by the Agilisys/Sefton Council Joint Information Security Forum and the Agilisys Security Steering Committee.
- Based on existing controls and residual risk, either accept the risk or agree on a treatment action (i.e. reduce, transfer, or avoid), which will be added to the Risk Treatment Plan. All risk actions taken by the information asset owner must be reviewed by the Agilisys/ Sefton Council Joint Information Security Forum and the Agilisys Security Steering Committee.
- The Risk Treatment Plan will be reviewed on an on-going basis by the Agilisys/Sefton Council Joint Information Security Forum and the Agilisys Security Steering Committee.

2.2 Risk Reporting and Acceptance

The Agilisys/Sefton Council Joint Information Security Forum will determine:

- The appropriate approach to align the Agilisys and the Council's risk processes to ensure consistent definitions (impact, likelihood);
- The severity at which risks are escalated to the Council and the forum through which this will be done;
- Who will own risks within the Agilisys and the Council's organisations and the criteria for acceptance of residual risk.

3 Security Policy

3.1 Agilisys Security Policies

The policies governing the ISMS will be the Agilisys Information Security Policy and related documents.

The Information Security Policy describes the organisation's approach to information security as well as approved mandatory information security controls based on the Statement of Applicability.

The Agilisys Security Steering Committee will review the Agilisys Information Security Policy and related documents to ensure that they remain up to date with changes in legislation, regulation, technology and business approach, and that they constantly reflect and support the control environment approved by Agilisys.

All approved changes to policy will be communicated to all affected personnel via normal communication channels and updated policies will be provided on the Agilisys intranet where they will be accessible to all personnel.

All personnel must sign the Agilisys Information Security Policy appropriate to their employment terms prior to being granted access to Agilisys or customer information processing systems. This will be recorded. All personnel will be required to re-read the Agilisys Information Security Policy at determined intervals during their employment.

3.2 Sefton Council's Security Policies

There may be instances where a Council Information Security Policy or related documents contains requirements for Agilisys employees working in that Council environment, which differ from the Agilisys Information Security Policy. In such instances, normally identified during transition, the following should be considered by the Agilisys Security Steering Committee and the Agilisys/ Sefton Council Joint Information Security Forum:

- Whether the Council's policies or "standard" Agilisys policies take precedence;
- The best approach if a Council's security policy requirement exceeds the equivalent Agilisys requirement;
- The best approach to conduct a gap analysis between the policy sets and record the results;
- The best approach to guarantee Agilisys receives all updates to the Council's supplied policies.

4 Organisation of Information Security

4.1 Agilisys Governance Structure

The ISMS will describe in detail the security governance model for Agilisys Services provided to the Council and how the model will be implemented in the parts of Agilisys within the scope of the ISMS. As part of the governance structure Agilisys has established the Agilisys Security Steering Committee (SSC) which actively supports security within the organisation through clear direction and demonstrated commitment.

4.2 Account Governance Structure

For services Agilisys will provide to the Council, to be agreed with the Council through the Agilisys/ Sefton Council Joint Information Security Forum, the following approach is specifically to be applied:

- Definition of key security roles and responsibilities for the Agilisys account team and where those roles are leveraged from the Agilisys Group (e.g. corporate or shared services)
- Definition of key security roles and responsibilities for the Council's organisation (e.g. CISO, SIRO and Head of Design Authority)
- Representation at the Council's Technical Design Authority and Change Board
- Membership and Terms of Reference for Agilisys/ Sefton Council Joint Information Security Forum

An Agilisys/ Sefton Council Joint Information Security Forum will be established for the ISMS, which will meet on a quarterly basis to review the performance of the ISMS and recommend improvements. This Joint Information Security Forum will consist of senior personnel from Agilisys and the Council and will be chaired by an Agilisys Information Security Manager.

The Joint Information Security Forum will report to the Council and Agilisys senior management via those organisations' governance structures.

4.3 External parties

Third Parties will be rigorously controlled to maintain the security of the Council's information and information processing facilities by third parties.

Controls will identify:

- The 3rd party organisations which form part of the supply chain for services Agilisys delivers to the Council;
- What services and/or products those 3rd parties supply;
- What security certifications (or other assurance mechanisms) they offer (e.g. ISO27001, SOC2 type 2 reports, IASME etc.);
- Whether their contracts will be novated to Agilisys;
- The mechanisms to assess the effectiveness of their security controls;
- The security metrics they report, how often and in what form;
- The governance arrangements (e.g. conference calls, monthly meetings) and ownership for those;
- Whether Agilisys and/or the Council have a right of audit and, if so, how it will be exercised.

The details described above refer to those suppliers, service providers and vendors **previously engaged by the** Council to deliver part of the services transferring to Agilisys control.

Where Agilisys engage suppliers, service providers or vendors as part of the proposed solution, then responsibility for defining equivalent requirements during the vendor selection process will rest with Agilisys but will be discussed and agreed with the Council.

5 Asset Management

5.1 Inventory of Assets

Agilisys will clearly identify all assets which will fall under the scope of the ISMS. Agilisys will identify and nominate an owner to maintain and protect the assets. Based on the importance of the asset, its business value, security classification, an appropriate level of protection will be identified.

Agilisys will deploy an appropriate software tool (where required) to create and periodically revalidate the register of physical assets.

Other information assets which are required for business continuity purposes (such as power supplies, communication services etc.) will be identified and recorded in a Business Continuity Plan.

5.2 Information Classification, Labelling and Handling

Agilisys will classify information in terms of its value, legal requirements, sensitivity and criticality to the Council. Agilisys will also establish a procedure for information labelling and handling according to the classification scheme adopted by the Council.

Agilisys will work with the Council to agree and document Information Assets falling within the scope of the services provided. Agilisys will populate an Information Asset Register to:

- Identify the information asset and its associated Information Asset Owner (IAO);
  Record the Protective Marking (PM), currently understood to be OFFICIAL, and that some may carry the OFFICIAL-Sensitive marking

5.3 Data Protection

For the purposes of the Data Protection Act 1998 and the EU General Data Protection Regulation (replacing the DPA in May 2018), the Council will be the Data Controller and Agilisys will be the Data Processor for all processing of Personally Identifiable Information (PII) and Sensitive Personable Information (SPI), including personal data stored in relevant Filing Systems and Accessible Public Records which are in scope.

Agilisys will process personal data in accordance with explicit instructions provided by the Council and detailed in the contract.

Agilisys will not host, process or access information from outside the European Economic Area

During the mobilisation phase, Agilisys will work with the Council to agree Agilisys responsibilities (if any) for the following:

- Breach notification;
- Responding to Subject Access requests;
- Responding to Freedom of Information requests;
- Conducting Privacy Impact Assessments and Legal or Data Protection compliance checks;
- Supporting the Council in the event of an Information Notice, Enforcement Notice or compulsory audit.

Changes to data protection requirements arising out of proposed EU regulations will be subject to agreement through the Agilisys/ Sefton Council Joint Information Security Forum and will be subject to change control.

6 Human Resources Security

Human Resources security controls will be established and deployed according to standards, guidelines and procedures, with due regard for ISO 27001 controls and in accordance with the security controls selected for this purpose.

Standard human resources security measures are in place within Agilisys, and these apply to all personnel providing services within scope of the ISMS. These measures include, but are not limited to:

- Pre-Employment Screening - taking into consideration requirements of the Council in regards to the HMG Baseline Personnel Security Standard process, UK Government (SC/DV) clearance requests, CTC, CRB/DBS and other checks;
- Signature of Information Security Policy during Induction;
- Information Security Awareness Training for all staff including contractors and agency staff;
- Terms and Conditions of Employment (including provisions for confidentiality of customer information);
- Starters/Movers/Leavers Procedures ensuring that all user access is
    - in line with job role
    - appropriately authorised by manager/team leader
    - subject to regular review to ensure that access remains relevant
- Disciplinary Procedures for Policy Violations.

6.1 Security Awareness Education

Mandatory Information Security Awareness Training will be provided to all Agilisys personnel. Additionally, enhanced Data Protection Act Awareness training will be provided to Agilisys personnel who are likely to encounter process or manage personal data during the course of their duties. The effectiveness of Information Security and Data Protection Act Awareness Training will be measured by means of a test upon completion of the training material.

Information Security Awareness Training and Data Protection Act Awareness Training will be repeated on a regular basis (at least annual), in order to ensure that awareness levels are maintained and that employees are provided with up to date guidance.

Agilisys outlines for its employees:

- What security responsibilities they have;
- What documents they must read and by when;
- What security training they must undertake and by when;
- How to report incidents and where to get advice;
- How this is linked to the disciplinary process.

7 Physical and Environmental Security

Physical and Environmental security controls will be established and deployed according to standards, guidelines and procedures, with due regard for ISO 27001 controls in accordance with the security controls selected for this purpose.

7.1 Agilisys Operated Sites

Access to sites managed by Agilisys will be controlled by way of entry/exit controls, and the following policies will be implemented by Agilisys in relation to office and/or datacentre sites, in addition to standard Health and Safety controls:

- Ingress and Egress Control;
- Addition and Removal of Equipment;
- Clear Desk / Workspace;
- Personnel Identification Badges;
- Equipment Security;
- Secure disposal of equipment;
- Escorting of Third Parties and Visitors;
- Environmental Controls;
- Hazard Controls (Fire and Flooding).

Agilisys will ensure that all Council data including protectively marked and personally identifiable information, wherever processed or stored by Agilisys is physically protected from accidental or deliberate loss and/or destruction arising from environmental hazards such as fire or flood.

Agilisys will ensure that all Council data including protectively marked and personally identifiable information, wherever processed or stored by Agilisys is held on premises that are adequately protected from unauthorised entry and/or theft of such items. Agilisys will ensure that all locations used to provide the Services are physically secure including, where appropriate, through the use of burglar alarms, security doors, controlled access systems, etc.

Additional policies and physical security measures will be implemented where risk assessments, audits or incidents indicate a requirement for greater control.

7.2 Sefton Council Sites

For services Agilisys provides to the Council, to be agreed with the Council through the Agilisys/ Sefton Council Joint Information Security Forum, the following approach is specifically to be applied:

- Define the Council locations to be included within the scope of the ISMS and the duration of their inclusion (i.e. if equipment is to be migrated to an Agilisys Data Centre), or confirm the controls to be applied if the locations are outside of the ISMS;
- Identify the details, if applicable of any 3rd party facilities management operations;
- Agree the arrangements during transition for assessing existing physical access controls
- Document transitional arrangements for transfer of physical access management to Agilisys, including procedures for escorted/unescorted access to the Council's sites

8 Communications and Operations Management

8.1 Documented Operating Procedures

Formally documented operational procedures will be established to ensure the correct and secure operation of information systems. Detailed procedures will be established for the management of system failures. These will include the development of comprehensive contingency plans for critical information systems.

8.2 Change Management

Significant, non-routine changes to information processing facilities (hardware, software or procedure) will be subject to formal change control.

An appropriate and proportionate security assessment and risk analysis will be performed on each proposed change to the Services that are processed in accordance with the Contract Change Control Policy. Change details will be communicated to all relevant persons prior to implementation. Appropriate Security personnel will be represented at the Change Board.

8.3 Segregation of Duties

Agilisys will maintain segregation of duties, such that the management and execution of duties or areas of responsibility are separated, reducing the opportunity for misuse or unauthorised alteration of information or service.

The need for segregation of responsibilities and access entitlements will be identified and catalogued through the risk assessment process and appropriate segregation of duties rules will be enforced through the user administration process.

8.4 Separation of Development and Operational Facilities

Agilisys will separate operational, test and development environments as necessary to prevent operational problems such as accidental change or unauthorised access to operational software and business data.

8.5 Protective Monitoring

Agilisys will review the Service related audit trails produced in accordance with the Security Standards, Security Guidelines and Security Procedures and will produce a summary of the logs in monthly reporting.

Agilisys will notify the Council of any unusual or anomalous activities identified and any potential security events will be managed as defined in the Security Incident Management process. Agilisys will apply adequate controls to protect and log information against unauthorised changes and operational problems, and retain events which may be relevant to future investigation for 6 months or a period of time as specified by the Council.

Subject to the Council commissioning the Security Operations Centre, further monitoring will be implemented and agreed with the Council to include the following capability:

The service provides comprehensive security visibility and is critical in uncovering security breaches; providing a holistic view of events across customer networks and reflects the need to identify security incidents at various touch points. The components that provide this are as follows:

- Log Management & SIEM
- SIEM/Event Correlation - When an incident happens CNS is able to provide immediate visibility into who, what, when, where, and how of the attack.
- Threat Management
    - Advanced Threat and Malware Detection

    - Known and Unknown Malware Detection
    - Web Based Attack Detection
    - Open Threat Exchange (OTX)
- Intrusion Detection Systems (IDS)
    - Network IDS – Identifies the latest attacks, malware infections, system compromise, policy violations, and other exposures.
    - Host IDS – monitors customer servers and applications for malicious activity and other unauthorised use of host resources
- Vulnerability Management
    - Vulnerability Assessment, Remediation, Scanning and Reporting – Designed to proactively identify weaknesses in the security posture of their IT estate.
- Network Security Monitoring
- Asset Discovery and Inventory - Provides visibility to the assets on customer's networks
- Behavioural Monitoring
- Log Collection – Essential for spotting unknown threats. It's also useful in investigating suspicious behaviour and policy violations
- Network Flow Analysis – Provides the high-level trends related to what protocols are used, which hosts use the protocol, and the bandwidth usage

8.6 Protection against Malicious Code

A standard solution will be deployed to protect against malware and other forms of malicious code on:

- Servers;
- Workstations;
- Other end-user devices; and
- Email communications.

Agilisys will also implement procedures and responsibilities to deal with malicious code to protect systems and aid recovery from malicious code attacks.

8.7 Backup and Recovery

Agilisys will provide adequate back-up services to minimise the risk of loss of or damage to the Council's Data and/or confidential information that it is responsible for storing, and ensure that a robust business continuity plan is in place in the event of restriction of Services for any reason.

To maintain the integrity and availability of information and information processing facilities, procedures will be established for the correct backup of systems and data. The procedures will address:

- Recovery requirements (e.g. Recovery to last backup, recovery to point of failure)
- Backup frequency
- Backup media
- Encryption of backup sets, including procedures for management and distribution of encryption keys
- Security of off-site storage of backup media and
- Periodic testing of the recovery process.

8.8 Network Security Management

Agilisys will implement adequate controls to safeguard information in networks and other supporting infrastructure.

Necessary controls will be implemented to safeguard confidentiality and integrity of data passing over public networks or over wireless networks. No connection to the corporate communications network will be permitted without obtaining the necessary authorisation.

Appropriate processes for responding to and maintaining codes of connection will be agreed with the Council.

8.9 Media handling

Agilisys will establish adequate controls to prevent unauthorised disclosure, modification, removal and destruction of information. These will include but not be limited to removable media controls, full hard drive encryption, and secure storage of media and secure disposal.

When information or software is to be transported, for instance via post, courier or electronically, appropriate controls will be applied to safeguard it. Operational procedures will be established to protect computer media and sensitive documentation from the possibility of damage, theft and unauthorised access.

Agilisys will not under any circumstances store the Council's data and/or confidential information on portable media or devices such as laptops, USB memory sticks or CD-ROMs unless agreed in writing by the Council 's representative and the Service Provider's Representative.

Agilisys will ensure that all portable media used for storage or transit of the Council's data and/or confidential information is fully encrypted in accordance with the Council's approved secure sharing methods.

Agilisys will only make printed paper copies of the Council's data and/or confidential information if this is essential for delivery of the Services in accordance with the terms of the Contract.

Agilisys will store printed paper copies of Council data and/or confidential information in locked cabinets when not in use and will not remove them from Council's premises unless this is essential for delivery of the Services in accordance with the terms of the Contract.

8.10 Disposal

Prior to disposal (for destruction or re-allocation) equipment and removable media will be handled in accordance with the Council's Corporate Procedure for the Disposal of IT Equipment and current CESG guidance. Facilities will be available for the secure destruction of magnetic media, in accordance with current CESG guidance.

Agilisys will ensure that Council data and/or confidential information held in paper form (regardless of whether as originally provided by the Council or printed from the Service Provider's IT systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company that complies with European standards.

Agilisys will provide the Council with copies of all relevant overwriting verification reports and/or certificates of secure destruction of the Council's data and/or confidential information following reasonable request from the Council at any time during this Contract and following the expiry and/or termination of this Contract.

8.11 Information Exchange agreement

When deemed necessary the physical and electronic exchange of any software or data between Agilisys and external bodies shall be subject to a formal agreement. Such agreements will include the identification data formats, secure carrier arrangements and process regarding verification of receipt.

8.12 Electronic messaging

Agilisys will apply the necessary controls where necessary, to reduce the business and security risk associated with electronic mail.

Agilisys will not transmit Council data and/or confidential information by email except as an attachment using the Council's approved secure sharing methods

- Secure email;
- One-off secure file transfer;
- Frequent secure file transfer;
- Secure post.

8.13 Clock Synchronisation

Agilisys will use agreed accurate time source to synchronise clocks of all relevant information processing systems within the organisation.

9 Access Control

9.1 Business requirement for access control

Access to computer services and data will be controlled on the basis of the business requirements.

Procedures will be established to control access to computer systems and data. These procedures will take full account of policies for the dissemination of, and entitlement to access corporate data.

Steps will be taken to make users aware of their responsibilities for maintaining effective system access controls, particularly regarding the use of user accounts, passwords and the security of information systems.

9.2 Documented access control policy

Business requirements for access control will be defined and documented. Agilisys will restrict access to information systems to only those staff and contractors who require such access to enable them to undertake their duties.

Agilisys will implement access controls in accordance with policies as follows:

- For Agilisys staff and contractors engaged in delivering the service to the Council, Agilisys will develop an access control policy, including Separation of Duties (SoD) rules for approval by the Agilisys/ Sefton Council Joint Information Security Forum.
- Where Agilisys is responsible, as part of the service to be delivered, for managing access for Council staff, then Agilisys will implement the access control policy, including Separation of Duties (SoD) rules defined by the customer.
- Agilisys will ensure that all access controls and associated mechanisms are hosted within the UK and managed and administered by UK staff. Full monitoring of access shall be facilitated from the UK by UK staff.

9.3 User access management

Agilisys will implement formal user registration and de-registration procedures for granting and revoking access to all information systems and services. The procedures will be established for privileged account management and review of user access rights. Agilisys will impose strong password guidelines which are set out in ‘Agilisys password guideline’ document.

9.4 User responsibilities

Agilisys will educate all staff to use strong passwords for all information systems. Agilisys will impose Clear Desk policy to all staff unless specified otherwise by the Council. These guidelines will be distributed to all users within the organisation.

9.5 Network access control

Access to both internal and external networked services will be controlled. This is necessary to ensure that users that have access to Agilisys network do not compromise their security. Agilisys will implement procedures for network services access control. Adequate controls and procedure will be established for remote connectivity and authentication.

10 Systems Acquisition, Development and Maintenance

10.1 Acquisition

New systems or software acquired will comply with the security policy as defined in this document and Agilisys technical standards. Exceptions to the security policy and associated risk will be referred to the Security Steering Group, to consider a waiver or for the security policy to be revised, if required. Where a waiver is proposed it will be agreed with the Agilisys/ Sefton Council Joint Information Security Forum

10.2 Systems Development

Software development will use appropriate tooling to enforce configuration control. Configuration control shall apply across development, test and production environments. Changes shall conform to the agreed Change Management Process.

10.3 Application Security

The IT systems may include software components that range from the operating system level, up through middleware (e.g. message handling) through to the applications that are visible by internal operational staff and external Council staff.

A procedure will be introduced so that the authentication processes for end users are reviewed to consider alternative technologies. The review will be conducted annually or when requested by the Agilisys/ Sefton Council Joint Information Security Forum and will make recommendations, which will then be subject to change control procedures.

10.4 Cryptographic Controls and Key Management

In order to protect the confidentiality, integrity and availability of information, a policy will be developed to address the use of cryptographic controls, based on a risk assessment and an assessment of costs and benefits. The standard will address:

- Where cryptographic controls will be used (removable media, data in transit, data at rest, wireless connection, mobile devices);
- The type, strength and quality of cryptographic algorithm required by the Business Impact level of the information;
- Management, distribution, recovery and revocation of key materials; and
- Legislative or regulatory restrictions on the use of cryptographic techniques.

10.5 System Maintenance

Changes to the production environment will be reviewed and approved in accordance with the Change Management Process. The process includes an impact assessment of the proposed change and other measures such as patch and vulnerability management, patch testing, security configuration against security policies after upgrades.

11 Information Security Incident Management

Information security incidents will be handled according to Agilisys Security Incident Management Process. A procedure will be established and agreed with the Council for logging and analysing security incident events and weaknesses.

All information security incidents will be recorded and reported to management for a formal review and root cause analysis. Agilisys will notify the nominated incident handling point of contact upon becoming aware of a security incident within agreed timescales.

Agilisys will:

- Categorise the incident as low, medium or high;
- React to the incident, taking the appropriate action in accordance with the Agilisys Security Incident Management Process, and as agreed with the Council;
- Notify the nominated incident handling point of contact within the Council where the incident is categorised as medium or high

11.1 Forensic Readiness

In cases where prosecution or disciplinary action may be required, information relating to the incident will be preserved as evidence. Agilisys do not provide forensic services but will be prepared to provide information as appropriate to contractual obligations should the Council engage a forensics service.

Agilisys and the Council will agree the process for the Council to notify Agilisys if a forensic process is required to support an investigation. Considerations will include:

- Defining Agilisys' role in forensic investigations;
- Agreeing the information Agilisys will need to provide in "first responder" capability;
- Deciding whether (and how) Agilisys/the Council will handle seizure of systems and/or mobile devices (including BYOD devices)
- Agreeing the Agilisys obligations for providing witnesses for the Council's internal tribunals and prosecutions;
- Agreeing the responsibilities Agilisys will have for handling RIPA notifications.

11.2 Security Incident Process Integration

For services Agilisys provides to the Council, we will discuss and agree with the Council through the Agilisys/ Sefton Council Joint Information Security Forum:

- How Agilisys will integrate the incident management process with the Council and any critical 3rd parties;
- How Agilisys/Sefton will test the integrated process;
- How Agilisys/Sefton will train incident handlers, especially first responders.

12 Business Continuity Management

Business continuity will be managed according to the functional requirements of the parts of the organisation within the scope of the ISMS.

Agilisys will ensure that all business continuity and disaster recovery plans are regularly tested and updated. Business continuity and disaster recovery tests are to occur at least once every 12 months. The Council will be notified in advance of the business continuity and disaster recovery plan testing schedule, and may appoint internal or external personnel to witness and contribute to the test procedure.

Availability considerations in forming the Business Continuity Plan include:

- The Agilisys Service Desk must be available during the contracted hours;
- All other Agilisys services will be subject to Recovery Time Objectives (RTO) defined in Service Level Agreements (SLAs).

For the Council this Plan will describe the following:

- How Agilisys will integrate the business continuity process with the Council and any critical 3rd parties;
- How Agilisys/Sefton will test the integrated process;
- How Agilisys will be represented on the Council's Crisis Management Team, in relation to services provided to the Council by Agilisys;
- Who, from Agilisys, has the authority to declare a major incident and initiate the switch to Disaster Recovery (DR)

Results of business continuity and disaster recovery tests will be reviewed by Agilisys after the tests have taken place. Comments and requests for Changes to business continuity and disaster recovery plans will be managed via corrective and preventive action procedures, in accordance with ISO 27001.

The results of each test are to be recorded in the Information Security Management System (ISMS), possible improvements identified and implemented, and the minutes of business continuity tests should be reviewed by the Agilisys Security Steering Committee and the Agilisys/ Sefton Council Joint Information Security Forum periodically.

13 Compliance

13.1 Applicable legislation

Agilisys will, in co-operation with the Council and legal counsel, determine the applicable legislation and EU Directives that apply to the environment as well as the levels of compliance required.

These legislative requirements will include, but are not limited to:

- Data Protection Act 1998
- EU General Data Protection Regulation
- Freedom of Information Act 2000
- Human Rights Act
- Regulation of Investigatory Powers Act 1999
- Computer Misuse Act
- Lawful Business Practices Regulations 2000

Agilisys will regularly verify compliance with applicable legislation and EU Directives via internal audits of the environment and personnel who access the environment.

The Agilisys/ Sefton Council Joint Information Security Forum will be responsible for maintaining a comprehensive list of the Council's statutory, regulatory and contractual requirements. These will also be recorded by the Agilisys Security Steering Committee.

13.2 Security Compliance Monitoring

Agilisys will track and advise the Council of non-compliance with the Security Standards, Security Policies and Security Processes. Where the non-compliance is within Agilisys' control, Agilisys will identify the reasons for non compliance and put in place remedial measures to prevent any recurrence.

13.3 Safeguarding Organisational records

The Agilisys/ Sefton Council Joint Information Security Forum will be responsible, through the data classification policy for the assessment of compliance requirements and defining recording requirements for information assets, including the retention period. This information will be considered, when planning to retire applications or systems and when establishing or modifying archiving procedures.

In particular, sufficient organisational records will be retained to fulfil the customer's obligations to respond to requests furnished under:

- Data Protection Act 1998
- EU General Data Protection Regulation
- Freedom of Information Act 2000
- Computer Misuse Act
- RIPA (1999)
- Lawful Business Practices regulations 2000
- HRA.

Responsibility for defining the retention requirements for all information assets rests with the Council. The Agilisys/ Sefton Council Joint Information Security Forum will be responsible for maintaining record retention schedules to meet the obligations of both the Council and Agilisys Records Management Policies.

13.4 Regulation of Cryptographic Controls

The Agilisys Security Steering Group and the Agilisys/ Sefton Council Joint Information Security Forum will be responsible for determining compliance requirements to national legislation, regulations, agreements and other requirements, relating to the use of cryptographic controls. Controls will be implemented to enable compliance with identified regulations.

13.5 Compliance with security policies and standards

Agilisys will ensure that all activities within the organisation are carried out correctly to achieve compliance with the security standards, guidelines and procedures. Internal audit will be used and results of audit and corrective actions will be recorded and maintained.

Agilisys will perform a regular annual audit of the technical design to ensure it continues to reflect good security practice, taking into account any new and emerging threats and new technologies.

Agilisys will be compliant with ISO 27001 and will undertake a regular annual audit of processes and procedures to ensure they continue to comply with the standard.

13.6 Technical compliance checking

Agilisys will conduct technical compliance checking either by following manufacturers' good practice guidelines, or system hardening documents. Agilisys will also conduct penetration testing and vulnerability assessment to meet legislative and contractual requirements.

- Quarterly internal security testing where required for PCI DSS compliance
    - Testing should at least include a review of internal hardware infrastructure to identify weak configurations, unsupported software and operating system versions and missing security patches.
- Annual external security testing by a qualified CHECK or CREST (or equivalent) independent tester
    - Testing should at least include a review of externally facing infrastructure and services to identify weaknesses with design, implementation and configuration that may allow compromise of that infrastructure or the networks, infrastructure and services behind it.

13.7 Information systems audit consideration

Periodic audits of working practices will be undertaken to ensure compliance with the Agilisys Information Security Management System. The purpose and scope of each audit study and the procedures to be used will be agreed with the person responsible for the area or system which is subject to audit. Auditors will only be given access to the software and data on the systems which are subject to audit, except where this is not practical due to technical limitations e.g. processing data on PC equipment.

Auditors will be provided with the resources required for audit purposes, except where this would endanger delivery of service of the system subject to audit. Auditors will be required to log all their access to systems, and the procedures they have employed during audit. All system audit software and data files will be separated from development and operational systems and will be accessible only to the Council's audit function.

The Agilisys Information Security Team will arrange a continual review of operational information systems to ensure that security controls have been properly implemented and continue to be effective.

14 Document Control

Revision History

Version	Date	Amended By	Summary of changes
0.1	10/04/2018	Simon Pilgrim	First draft
0.2	31/08/2018	Steve Morgan	Updates after initial review

Document Approval

This document requires the following approvals. ('Approved' assumes review undertaken prior to approval).

Version	Date	Name	Title / Role	Approval Status (Pending/Approved)
0.1	10/04/2018	Rob Alcock	Service Director	Approved
0.1	10/04/2018	Steve Morgan	Partnership Director	Approved
0.2	04/09/2018	Rob Alcock	Service Director	Approved
0.2	04/09/2018	Mark Wishart	Arvato Security Officer	Pending
0.2	04/09/2018		Sefton Council	Pending

Document Reviews

This document has been reviewed by the following people, in addition to those listed above.

Version	Date	Name	Title / Role
0.1	10/04/2018	Steve Morgan	Partnership Director